AMENDMENT TO THE CLAIMS:

This listing of claims will replace all prior versions of claims in the application.

Listing of Claims:

1-14. (Cancelled)

15. (Currently Amended) A process for the remote authentication of a user for local access to a local machine of a network having a remote server managed by an administrator ~~and~~, classification means for classifying information, and communication means for connecting the user and the administrator comprising:

creating a challenge (D) capable of being transmitted by the communication means, the challenge including information representing the type of challenge, version information and alphanumeric characters, the type of challenge representing whether a network authentication has been performed;

communicating the challenge (D) to the administrator together with elements known by the user, via the communication means;

performing a first predetermined calculation by means of the server and obtaining a first response (RD) that is a function of at least one of the challenge (D) and of predetermined data;

transmitting to the user by the administrator the first response (RD);

performing a second calculation by means of the local machine and obtaining a second response (RD1) that is a function of at least one of the challenge (D) and of the predetermined data; and

comparing the first response (RD) transmitted by the administrator to the second response (RD1) ~~calculated~~ obtained by the local machine so as to authenticate the user and locally authorize connection of the user to the local machine based on the result of the comparison.

16. (Previously Presented) A process according to claim 15, wherein the first predetermined calculation performed by the server comprises modifying, in accordance with a given algorithm, the challenge (D) and at least one of the following pieces of data:

a.) at least one piece of information issued by the classification means and known by the user,

b.) at least one secret shared between the server and the local machine, and

c.) at least one element communicated by the user.

17. (Previously Presented) A process according to claim 15, wherein the second calculation performed by the local machine comprises modifying, in accordance with a given algorithm, the challenge (D) and at least one of the following pieces of data:

a.) at least one secret shared between the server and the local machine, and

b.) at least one element communicated by the user.

18. (Currently Amended) A process according to claim 16, wherein the second calculation performed by the local machine comprises modifying, in accordance with a given algorithm, the challenge (D) and at least one of the following pieces of data:

a.) at least one secret shared between the server and the local machine, and

b.) at least one element communicated by the user.

19. (Previously Presented) A process according to claim 16, wherein said at least one shared secret is entered into the server and transmitted to the local machine during a successful network authentication.

20. (Previously Presented) A process according to claim 17, wherein said at least one shared secret is entered into the server and transmitted to the local machine during a successful network authentication.

21. (Previously Presented) A process according to claim 18, wherein said at least one shared secret is entered into the server and transmitted to the local machine during a successful network authentication.

22. (Previously Presented) A process according to claim 16, wherein said at least one shared secret or secrets, as the case may be, are modified by means of a modification key (C) that depends on the local machine, prior to being modified by the algorithm.

23. (Previously Presented) A process according to claim 22, wherein the modification key (C) comprises concatenating the secret or a combination of secrets existing in the form of a byte string called a Master Station Secret and of hashing the byte string obtained through concatenation by means of a calculation algorithm, to obtain a byte string called a Station Secret.

24. (Previously Presented) A process according to claim 16, wherein said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

25. (Previously Presented) A process according to claim 17, wherein said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

26. (Previously Presented) A process according to claim 18, wherein said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

27. (Previously Presented) A process according to claim 15, wherein the challenge is constituted by a byte string.

28. (Previously Presented) A process according to claim 16, wherein the challenge is constituted by a byte string.

29. (Currently Amended) A process for the remote authentication of a user for local access to a local machine of a network having a remote server managed by an administrator ~~and~~, classification means for classifying information, and means for connecting the user and the administrator comprising:

creating a challenge (D) capable of being transmitted by the communication means;

communicating the challenge (D) to the administrator together with elements known by the user, via the communication means;

performing a first predetermined calculation by means of the server and obtaining a first response (RD) that is a function of at least one of the challenge (D) ~~and/or~~ and of predetermined data;

transmitting to the user by the administrator the first response (RD);

performing a second calculation by means of the local machine and obtaining a second response (RD1) that is a function of at least one of the challenge (D) ~~and/or~~ and of the predetermined data; and

comparing the first response (RD) transmitted by the administrator to the second response (RD1) ~~calculated~~ obtained by the local machine so as to authenticate the user and locally authorize connection of the user to the local machine based on the result of the comparison,

wherein the first predetermined calculation performed by the server comprises modifying, in accordance with a given algorithm, the challenge (D) and at least one of the following pieces of data:

at least one piece of information issued by the classification means and known by the user,

at least one secret shared between the server and the local machine, and

at least one element communicated by the user; and

said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified; and

the challenge comprises:

a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed;

second and third bytes representing the version number of the shared information; and

random alphanumeric characters of the fourth to twelfth bytes.

30. (Currently Amended) A process for the remote authentication of a user for local access to a local machine of a network having a remote server managed by an administrator ~~and~~, classification means for classifying information, and means for connecting the user and the administrator comprising:

creating a challenge (D) capable of being transmitted by the communication means;

communicating the challenge (D) to the administrator together with elements known by the user, via the communication means;

performing a first predetermined calculation by means of the server and obtaining a first response (RD) that is a function of at least one of the challenge (D) ~~and/or~~ and of predetermined data;

transmitting to the user the first response (RD);

performing a second calculation by means of the local machine and obtaining a second response (RD1) that is a function of at least one of the challenge (D) ~~and/or~~ and of the predetermined data; and

comparing the first response (RD) transmitted by the administrator to the second response (RD1) calculated by the local machine so as to authenticate the user and locally authorize connection of the user to the local machine based on the result of the comparison, wherein,

the challenge comprises:

a byte string, comprising:

a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed;

second and third bytes representing the version number of the shared information; and

random alphanumeric characters of the fourth to twelfth bytes.

31. (Previously Presented) A process according to claim 23, wherein the response (RD; RD1) is calculated by hashing, in accordance with a calculation algorithm, a character string comprising the concatenation in a predetermined order of the challenge, the character string resulting from the transformation by a calculation algorithm of the user's password, the Station Secret and the user's name.

32. (Previously Presented) A process according to claim 15, wherein the response (RD; RD1) is calculated by hashing, in accordance with a calculation algorithm, a character string comprising the concatenation in a predetermined order of the challenge, a fixed security key CC stored in the local machine and in the server, the name of the local machine, and the character string resulting from the transformation by a calculation algorithm of the user's password and user name.

33. (Previously Presented) A process according to claim 15, wherein the local connection authorized is temporary, the authorized duration of the local connection being configurable.

34. (Previously Presented) A process according to claim 15, further comprising locally authenticating the user after the user authenticated remotely is disconnected from the local machine.

35. (Currently Amended) A system for the remote authentication of a local user for local access to a local machine of a network having a remote server managed by an administrator and containing means for classifying information, comprising communication means for connecting the user with the administrator, each local machine comprising a user authentication module that includes a first user module for generating a challenge, the challenge including information representing the type of challenge, version information and alphanumeric characters, the type of challenge representing whether a network authentication has been performed, and a second user module for calculating a response to the challenge, and the remote server comprising an administrative authentication module for authorizing access by the user to the local machine based on the response generated.